#3

THE COMMISSIONER IS AUTHORIZED TO CHARGE ANY DEFICIENCY IN THE FEES FOR THIS PAPER TO DEPOSIT ACCOUNT NO. 23-0975

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of :

Hisashi INOUE et al. :

Serial No. NEW : **Attn: APPLICATION BRANCH**

Filed November 21, 2000 : Attorney Docket No. 2000_1451A

APPARATUS AND METHOD FOR EMBEDDING INFORMATION FOR TAMPER DETECTION AND DETECTING TAMPER AND RECORDING MEDIUM HAVING PROGRAM FOR CARRYING OUT THE METHOD RECORDED THEREON

CLAIM OF PRIORITY UNDER 35 USC 119

Assistant Commissioner for Patents,
Washington, DC 20231

Sir:

Applicants in the above-entitled application hereby claim the date of priority under the International Convention of Japanese Patent Application No. 11-333775, filed November 25, 1999, as acknowledged in the Declaration of this application.

A certified copy of said Japanese Patent Application is submitted herewith.

Respectfully submitted,

Hisashi INOUE et al.

By _____
Charles R. Watts
Registration No. 33,142
Attorney for Applicants

CRW/asd
Washington, D.C. 20006
Telephone (202) 721-8200
Facsimile (202) 721-8250
November 21, 2000

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９９年１１月２５日

出 願 番 号
Application Number: 平成１１年特許願第３３３７７５号

出 願 人
Applicant (s): 松下電器産業株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年 ６月２３日

特許庁長官
Commissioner,
Patent Office 近藤隆彦

【書類名】　特許願

【整理番号】　2038610041

【提出日】　平成11年11月25日

【あて先】　特許庁長官殿

【国際特許分類】　H04N　1/387

G09C　5/00

G06T　9/00

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　井上　尚

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　桂　卓史

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100097445

【弁理士】

【氏名又は名称】　岩橋　文雄

【選任した代理人】

【識別番号】　100103355

【弁理士】

【氏名又は名称】　坂口　智康

【選任した代理人】

【識別番号】　100109667

【弁理士】

【氏名又は名称】　内藤　浩樹

【手数料の表示】

【予納台帳番号】　011305

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9809938

【プルーフの要否】　不要

【書類名】　明細書

【発明の名称】　デジタル画像の改ざん防止装置および方法並びに当該方法を実施するプログラムを記録した記録媒体

【特許請求の範囲】

【請求項１】　デジタル画像信号を複数の周波数帯域に分割する帯域分割手段と、予め定めた鍵データを用いて疑似乱数系列を作成し、当該疑似乱数系列から認証データを作成する認証データ作成手段と、前記複数の周波数帯域のうち、最も低い周波数帯域（以下、ＭＲＡという）の変換係数に前記鍵データを埋め込む鍵情報埋込み手段と、ＭＲＡ以外の周波数帯域（以下、ＭＲＲという）の変換係数に前記認証データを埋め込む認証データ埋込み手段と、情報埋め込み後の前記ＭＲＡと前記ＭＲＲを用いて、情報の埋め込みがなされたデジタル画像信号を再構成する帯域合成手段とを備えたことを特徴とする改ざん防止装置。

【請求項２】　デジタル画像信号を複数の周波数帯域に分割する帯域分割手段と、前記複数の周波数帯域のうち、ＭＲＡの変換係数から鍵データを抽出する鍵情報抽出手段と、前記鍵データを用いて疑似乱数系列を作成し、当該疑似乱数系列から認証データを作成する認証データ作成手段と、前記複数の周波数帯域のうち、ＭＲＲの変換係数から埋込み情報を抽出する埋込み情報抽出手段と、前記認証データと抽出した前記埋込み情報とを比較照合して改ざんの有無を判定する改ざん判定手段とを備えたことを特徴とする改ざん防止装置。

【請求項３】　正の数である第１の設定値および第１の設定値より小さい正の数を第２の設定値ｍとして予め定め、前記認証データ埋込み手段は、変換係数の絶対値と第１の設定値とを比較し、前記変換係数の絶対値が第１の設定値より小さい場合、変換係数に対応する認証データのビット値に応じて、前記変換係数をｍまたは－ｍに設定する第１の埋込み手段と、前記変換係数を量子化ステップサイズＱで割った値をｑとして予め定め、前記変換係数の絶対値が第１の設定値以上の場合、変換係数に対応する認証データのビット値に応じて、前記ｑの値を最も近い偶数または奇数の整数値に設定する第２の埋込み手段とを備え、前記認証データをＭＲＲの変換係数に埋め込むことを特徴とする請求項１に記載の改ざん防止装置。

【請求項４】　前記埋込み情報抽出手段は、変換係数の絶対値と前記第１の設定値とを比較し、前記変換係数の絶対値が前記第１の設定値より小さい場合、前記変換係数の値が正か負かを判定し、当該判定の結果に基づいて変換係数毎に埋込まれた情報のビット値を抽出する第１の抽出手段と、前記変換係数を量子化ステップサイズＱで割り四捨五入した値をｐとして予め定め、前記変換係数の絶対値が前記第１の設定値以上の場合、前記ｐの値が偶数か奇数かを判定し、当該判定の結果に基づいて変換係数毎に埋込まれた情報のビット値を抽出する第２の抽出手段とを備え、前記ＭＲＲの変換係数から埋込み情報を抽出することを特徴とする請求項２または３に記載の改ざん防止装置。

【請求項５】　前記改ざんの有無を判定する改ざん判定手段は、デジタル画像を予め定めた複数の画素から構成される複数のブロックに分割するブロック分割手段と、ブロックと同一の空間的領域を表現するＭＲＲ内に埋め込まれている埋込み情報の系列を前記抽出した埋込み情報の中から読み出す領域対応埋込情報読出手段と、前記認証データの中から、前記読み出した埋込み情報と同じ位置に対応する認証データの系列を読み出す領域対応認証データ読出手段と、前記ブロック毎に読み出された前記埋込み情報の系列と前記認証データの系列とを比較することによって、当該ブロックの改ざんの有無を判定するブロック改ざん判定手段とを備えたことを特徴とする請求項２に記載の改ざん防止装置。

【請求項６】　デジタル画像信号を複数の周波数帯域に帯域分割するステップと、予め定めた鍵データを用いて疑似乱数系列を作成し、当該疑似乱数系列から認証データを作成するステップと、前記複数の周波数帯域のうち、最も低い周波数帯域（以下、ＭＲＡという）の変換係数に前記鍵データを埋め込むステップと、ＭＲＡ以外の周波数帯域（以下、ＭＲＲという）の変換係数に前記認証データを埋め込むステップと、情報埋め込み後の前記ＭＲＡと前記ＭＲＲを用いて、情報の埋め込みがなされたデジタル画像信号を再構成するステップとを備えたことを特徴とする改ざん防止方法。

【請求項７】　デジタル画像信号を複数の周波数帯域に帯域分割するステップと、前記複数の周波数帯域のうち、ＭＲＡの変換係数から鍵データを抽出するステップと、前記鍵データを用いて疑似乱数系列を作成し、当該疑似乱数系列から

認証データを作成するステップと、前記複数の周波数帯域のうち、ＭＲＲの変換係数から埋込み情報を抽出するステップと、前記認証データと抽出した前記埋込み情報を比較照合して改ざんの有無を判定するステップとを備えたことを特徴とする改ざん防止方法。

【請求項８】　正の数である第１の設定値および第１の設定値より小さい正の数を第２の設定値ｍとして予め定め、前記ＭＲＲの変換係数に埋め込むステップは、変換係数の絶対値と第１の設定値とを比較し、前記変換係数の絶対値が第１の設定値より小さい場合、変換係数に対応する認証データのビット値に応じて、前記変換係数をｍまたは－ｍに設定するステップと、前記変換係数を量子化ステップサイズＱで割った値をｑとして予め定め、前記変換係数の絶対値が第１の設定値以上の場合、変換係数に対応する認証データのビット値に応じて、前記ｑの値を最も近い偶数または奇数の整数値に設定するステップとを備え、前記認証データをＭＲＲの変換係数に埋め込むことを特徴とする請求項６に記載の改ざん防止方法。

【請求項９】　前記ＭＲＲの変換係数から埋込み情報を抽出するステップは、変換係数の絶対値と前記第１の設定値とを比較し、前記変換係数の絶対値が前記第１の設定値より小さい場合、前記変換係数の値が正か負かを判定し、当該判定の結果に基づいて変換係数毎に埋込まれた情報のビット値を抽出するステップと、前記変換係数を量子化ステップサイズＱで割り四捨五入した値をｐとして予め定め、前記変換係数の絶対値が前記第１の設定値以上の場合、前記ｐの値が偶数か奇数かを判定し、当該判定の結果に基づいて変換係数毎に埋込まれた情報のビット値を抽出するステップとを備え、前記ＭＲＲの変換係数から埋込み情報を抽出することを特徴とする請求項７または８に記載の改ざん防止方法。

【請求項１０】　前記改ざんの有無を判定するステップは、デジタル画像を予め定めた複数の画素から構成される複数のブロックに分割するステップと、ブロックと同一の空間的領域を表現するＭＲＲ内に埋め込まれている埋込み情報の系列を前記抽出した埋込み情報の中から読み出すステップと、前記認証データの中から、前記読み出した埋込み情報と同じ位置に対応する認証データの系列を読み出すステップと、前記ブロック毎に読み出された前記埋込み情報の系列と前記認

証データの系列とを比較することによって、当該ブロックの改ざんの有無を判定するステップとを備えたことを特徴とする請求項７に記載の改ざん防止方法。

【請求項１１】　デジタル画像信号を複数の周波数帯域に帯域分割するステップと、予め定めた鍵データを用いて疑似乱数系列を作成し、当該疑似乱数系列から認証データを作成するステップと、前記複数の周波数帯域のうち、最も低い周波数帯域（以下、ＭＲＡという）の変換係数に前記鍵データを埋め込むステップと、ＭＲＡ以外の周波数帯域（以下、ＭＲＲという）の変換係数に前記認証データを埋め込むステップと、情報埋め込み後の前記ＭＲＡと前記ＭＲＲを用いて、情報埋め込みがなされたデジタル画像信号を再構成するステップを実行するためのプログラムを記録した記録媒体。

【請求項１２】　デジタル画像信号を複数の周波数帯域に帯域分割するステップと、前記複数の周波数帯域のうち、ＭＲＡの変換係数から鍵データを抽出するステップと、前記鍵データを用いて疑似乱数系列を作成し、当該疑似乱数系列から認証データを作成するステップと、前記複数の周波数帯域のうち、ＭＲＲの変換係数から埋込み情報を抽出するステップと、前記認証データと抽出した前記埋込み情報を比較照合して改ざんの有無を判定するステップを実行するためのプログラムを記録した記録媒体。

【請求項１３】　正の数である第１の設定値および第１の設定値より小さい正の数を第２の設定値ｍとして予め定め、前記ＭＲＲの変換係数に埋め込むステップは、変換係数の絶対値と第１の設定値とを比較し、前記変換係数の絶対値が第１の設定値より小さい場合、変換係数に対応する認証データのビット値に応じて、前記変換係数をｍまたは－ｍに設定するステップと、前記変換係数を量子化ステップサイズＱで割った値をｑとして予め定め、前記変換係数の絶対値が第１の設定値以上の場合、変換係数に対応する認証データのビット値に応じて、前記ｑの値を最も近い偶数または奇数の整数値に設定するステップとを備え、前記認証データをＭＲＲの変換係数に埋め込むことを特徴とする請求項１１に記載の記録媒体。

【請求項１４】　前記ＭＲＲの変換係数から埋込み情報を抽出するステップは、変換係数の絶対値と前記第１の設定値とを比較し、前記変換係数の絶対値が前

記第１の設定値より小さい場合、前記変換係数の値が正か負かを判定し、当該判定の結果に基づいて変換係数毎に埋込まれた情報のビット値を抽出するステップと、前記変換係数を量子化ステップサイズＱで割り四捨五入した値をｐとして予め定め、前記変換係数の絶対値が前記第１の設定値以上の場合、前記ｐの値が偶数か奇数かを判定し、当該判定の結果に基づいて変換係数毎に埋込まれた情報のビット値を抽出するステップとを備え、前記ＭＲＲの変換係数から埋込み情報を抽出することを特徴とする請求項１２または１３に記載の記録媒体。

【請求項１５】　前記改ざんの有無を判定するステップは、デジタル画像を予め定めた複数の画素から構成される複数のブロックに分割するステップと、ブロックと同一の空間的領域を表現するＭＲＲ内に埋め込まれている埋込み情報の系列を前記抽出した埋込み情報の中から読み出すステップと、前記認証データの中から、前記読み出した埋込み情報と同じ位置に対応する認証データの系列を読み出すステップと、前記ブロック毎に読み出された前記埋込み情報の系列と前記認証データの系列とを比較することによって、当該ブロックの改ざんの有無を判定するステップとを備えたことを特徴とする請求項１２に記載の記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、デジタル画像の改ざん防止装置および方法並びに記憶媒体に関し、より特定的には、デジタル画像の部分的な改ざんの有無及び改ざん位置を検出するために、デジタル画像信号に認証データを埋め込み、そして抽出する改ざん防止装置および方法並びに記憶媒体に関する。

【０００２】

【従来の技術】

近年、インターネットを利用した情報の提供が盛んになっている。特にＷＷＷ（Ｗｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ）は、画像や音声などを統合した情報送受信サービスとして頻繁に利用されている。しかしながら、こうしたオープンなネットワーク環境では、不特定多数の者が画像などのデジタル情報を容易にコピーすることができる。しかも、市販の画像処理ソフトウェアを利用して簡単にデジタル

画像を編集・加工することができ、デジタル画像が第三者によって改ざんされ、受信者は改ざんされたことに気付かれない場合が想定される。そこで、配信されたデジタル画像に改ざんが加えられているか否か判定できる改ざん検出技術の確立が求められている。従来、その対策の一つとして知られているものに電子認証技術がある。

【０００３】

図１４は、従来の電子認証の手順の概要を示した説明図である。送信側では、オリジナルのデジタル画像に対してハッシュ関数を適用してデータ圧縮したダイジェストを送り手による秘密鍵で暗号化する。そして、オリジナルのデジタル画像及び暗号化されたダイジェストをネットワークを通して受信側に送信する。受信側では、ネットワークより受信したデジタル画像に対してハッシュ関数によるデータ圧縮を行ってダイジェストを作成すると共に、暗号化されたダイジェストに対して送り手の公開鍵による復号化を行ってダイジェストを復号する。そして、オリジナルのデジタル画像から作成したダイジェストと復号したダイジェストとを比較し、両方のダイジェストが同一であれば改ざんが行われていないと判定し、逆に、異なっていれば改ざんが行われていると判定する。

【０００４】

ところが、上述のようにして電子認証を行う場合、送信側では、オリジナルのデジタル画像及び暗号化されたダイジェストの２種類のデータを受信側へ送信する必要があるが、デジタル画像が大量の場合には、ネットワークを通して送信する際に、どのデジタル画像に対してどのダイジェストが対応しているのかを送信側で適切に管理するためのデータ管理手段が別途必要になる。このようなデータ管理手段の代わりとして、従来、電子透かし技術を用いた手法がある。

【０００５】

電子透かしとは、デジタル画像データ内部に人間には知覚できないような形でデジタル情報を埋め込む技術である。電子透かし技術により、例えば、デジタル画像の上位ビットからダイジェストを作成し、これを送り手による秘密鍵で暗号化する。そして、デジタル画像の各画素の下位ビットに暗号化したダイジェストを埋め込む。受信側では送信されたデジタル画像の下位ビットに埋め込まれてい

る暗号化ダイジェストを抽出し、送り手の公開鍵による復号化を行ってダイジェストを復号する。一方、受信したデジタル画像の上位ビットから直接照合用ダイジェストを作成する。そして、照合用ダイジェストと復号したダイジェストとを比較し、両方のダイジェストが同一であれば改ざんが行われていないと判定し、逆に、異なっていれば改ざんが行われていると判定する。

【０００６】

【発明が解決しようとする課題】

しかしながら、従来の電子透かし技術では、送信途中でデジタル画像が改ざんされたことを受信側で発見できても、デジタル画像中のどの部分が改ざんされたかを特定することができないという課題があった。また、電子透かし方式では、一般に人間の目には知覚しにくい高周波成分を利用してダイジェストの埋め込みを行っているので、ＪＰＥＧなどの非可逆な画像圧縮伸長を行った場合、埋め込んだ情報が変化してしまい、正しく読み出せない。すなわち、悪意を持った者によるデジタル画像の一部を改変した場合と一般的に行う非可逆的な画像圧縮とによるデジタル画像の改ざんの区別ができないという課題があった。さらに、画像の高周波成分に対応する部分は、一般的にエッジやテクスチャ部分であるため、平坦な部分が多い画像では、画像全体に情報が埋め込まれないことになる。その結果、平坦部分を改ざんした場合は、検出できないことが発生する可能性がある。

【０００７】

それ故、本発明の目的は、画像の高周波成分だけではなく、画像全体に情報を埋め込む。すなわち、比較的低周波成分の変換係数に情報を埋込むことにより、非可逆的な圧縮と画像の一部を改ざんする行為とを区別することができ、しかも改ざん部分の特定が可能なデジタル画像の改ざん防止装置及び方法を提供することである。

【０００８】

【課題を解決するための手段】

第１の発明は、デジタル画像信号を複数の周波数帯域に分割する帯域分割手段と、予め定めた鍵データを用いて疑似乱数系列を作成し、当該疑似乱数系列から

認証データを作成する認証データ作成手段と、複数の周波数帯域のうち、最も低い周波数帯域（以下、ＭＲＡという）の変換係数に前記鍵データを埋め込む鍵情報埋込み手段と、ＭＲＡ以外の周波数帯域（以下、ＭＲＲという）の変換係数に前記認証データを埋め込む認証データ埋込み手段と、情報埋め込み後の前記ＭＲＡと前記ＭＲＲを用いて、情報の埋め込みがなされたデジタル画像信号を再構成する帯域合成手段とを備える。

【０００９】

第２の発明は、デジタル画像信号を複数の周波数帯域に分割する帯域分割手段と、前記複数の周波数帯域のうち、ＭＲＡの変換係数から鍵データを抽出する鍵情報抽出手段と、前記鍵データを用いて疑似乱数系列を作成し、当該疑似乱数系列から認証データを作成する認証データ作成手段と、前記複数の周波数帯域のうち、ＭＲＲの変換係数から埋込み情報を抽出する埋込み情報抽出手段と、前記認証データと抽出した前記埋込み情報とを比較照合して改ざんの有無を判定する改ざん判定手段とを備える。

【００１０】

第３の発明は、第１の発明に従属する発明であって、正の数である第１の設定値および第１の設定値より小さい正の数を第２の設定値ｍとして予め定め、変換係数の絶対値と第１の設定値とを比較し、前記変換係数の絶対値が第１の設定値より小さい場合、変換係数に対応する認証データのビット値に応じて、前記変換係数をｍまたは－ｍに設定する第１の埋込み手段と、前記変換係数を量子化ステップサイズＱで割った値をｑとして予め定め、前記変換係数の絶対値が第１の設定値以上の場合、変換係数に対応する認証データのビット値に応じて、前記ｑの値を最も近い偶数または奇数の整数値に設定する第２の埋込み手段とを備え、前記認証データをＭＲＲの変換係数に埋め込むことを特徴とする。

【００１１】

第４の発明は、第２または第３の発明に従属する発明であって、変換係数の絶対値と前記第１の設定値とを比較し、前記変換係数の絶対値が前記第１の設定値より小さい場合、前記変換係数の値が正か負かを判定し、当該判定の結果に基づいて変換係数毎に埋込まれた情報のビット値を抽出する第１の抽出手段と、前記

変換係数を量子化ステップサイズＱで割り四捨五入した値をｐとして予め定め、前記変換係数の絶対値が前記第１の設定値以上の場合、前記ｐの値が偶数か奇数かを判定し、当該判定の結果に基づいて変換係数毎に埋込まれた情報のビット値を抽出する第２の抽出手段とを備え、前記ＭＲＲの変換係数から埋込み情報を抽出することを特徴とする。

【００１２】

第５の発明は、第２の発明に従属する発明であって、デジタル画像を予め定めた複数の画素から構成される複数のブロックに分割するブロック分割手段と、ブロックと同一の空間的領域を表現するＭＲＲ内に埋め込まれている埋込み情報の系列を抽出した埋込み情報の中から読み出す領域対応埋込情報読出手段と、前記認証データの中から、前記読み出した埋込み情報と同じ位置に対応する認証データを読み出す領域対応認証データ読出手段と、前記ブロック毎に読み出された前記埋込み情報の系列と前記認証データの系列とを比較することによって、当該ブロックの改ざんの有無を判定するブロック改ざん判定手段とを備えたことを特徴とする。

【００１３】

【発明の実施の形態】

図１および図２は、本発明の実施形態に係るデジタル画像の改ざん防止装置の構成図である。図１は情報埋込み装置１ａを示すブロック図、図２は情報抽出装置２ａを示すブロック図である。

【００１４】

図１において、情報埋込み装置１ａは、帯域分割部１１と、認証データ作成部１２と、鍵情報埋込み部１３と、認証データ埋込み部１４と、帯域合成部１５とを備える。

【００１５】

図２において、情報抽出装置２ａは、帯域分割部１１と、鍵情報抽出部２１と、鍵情報判定部２２と、認証データ作成部１２と、埋込み情報抽出部２３と、領域対応埋込情報読出部２４と、領域対応認証データ読出部２５と、ブロック改ざん判定部２６とを備える。

【００１６】

なお、本実施形態に係る情報抽出装置２ａの帯域分割部１１と認証データ作成部１２は、本実施形態に係る情報埋込装置１ａの帯域分割部１１と認証データ作成部１２と同様の構成であり、以下当該構成について、同一の参照番号を付してその説明を省略する。

【００１７】

以下、図３～図１３を参照して、本実施形態に係るデジタル画像の改ざん防止装置が行う改ざん防止方法を順に説明する。

【００１８】

まず、情報埋込装置１ａが行う情報埋込み方法について説明する。図３は、図１の情報埋込み装置１ａで行う処理を示すフローチャートである。図３を参照して、まず、帯域分割部１１の処理について、図４～図６を用いて説明する。

【００１９】

図４は、従来の離散ウェーブレット変換処理を用いて３階層への帯域分割を行う帯域分割部１１の構成の一例を示すブロック図である。図４において、帯域分割部１１は、それぞれ同じ構成を有する第１～第３の帯域分割フィルタ１００、２００および３００を備える。第１～第３の帯域分割フィルタ１００、２００および３００は、入力した画像を４つの周波数帯域に分割し、各周波数帯域ごとのウェーブレット係数（以下、変換係数という）を算出する（ステップＳ３０１）。なお、サブバンド分割によっても、離散ウェーブレット変換による帯域分割と等価である変換係数を得ることもできる。帯域分割部１１は、デジタル画像信号７１を第１の帯域分割フィルタ１００に入力する。

【００２０】

第１の帯域分割フィルタ１００は、デジタル画像信号７１を水平周波数成分と垂直周波数成分のパラメータに基づいて４つの帯域の信号、すなわち、ＬＬ１信号、ＬＨ１信号、ＨＬ１信号およびＨＨ１信号（以下、これらを総称して第１の階層信号という）に分割する。

【００２１】

第２の帯域分割フィルタ２００は、上記第１の階層信号のうち最も低域のＬＬ

１信号を入力し、さらに４つの帯域のＬＬ２信号、ＬＨ２信号、ＨＬ２信号およびＨＨ２信号（以下、これらを総称して第２の階層信号という）に分割する。

【００２２】

そして、第３の帯域分割フィルタ３００は、上記第２の階層信号のうち最も低域のＬＬ２信号を入力し、さらに４つの帯域のＬＬ３信号、ＬＨ３信号、ＨＬ３信号およびＨＨ３信号（以下、これらを総称して第３の階層信号という）に分割する。

【００２３】

図５は、図４の第１の帯域分割フィルタ１００の構成の一例を示すブロック図である。図５において、第１の帯域分割フィルタ１００は、第１～第３の２帯域分割部１０１～１０３を備える。この第１～第３の２帯域分割部１０１～１０３は、それぞれ１次元の低域通過フィルタ（ＬＰＦ）１１１～１１３と、１次元の高域通過フィルタ（ＨＰＦ）１２１～１２３と、信号を２：１に間引くダウンサンプラ１３１～１３３および１４１～１４３とを備える。

【００２４】

第１の２帯域分割部１０１は、デジタル画像信号７１を入力し、水平方向成分に関してＬＰＦ１１１およびＨＰＦ１２１により低域および高域のフィルタリングを行い、２つの信号を出力する。そして低域および高域のフィルタリングがされた信号をそれぞれダウンサンプラ１３１および１４１を用いて２：１に間引いた後、次段に出力する。

【００２５】

第２の２帯域分割部１０２は、ダウンサンプラ１３１からの信号を入力し、垂直方向成分に関してＬＰＦ１１２およびＨＰＦ１２２によりそれぞれフィルタリングを行い、ダウンサンプラ１３２および１４２を用いて２：１に間引いた後、ＬＬ１信号とＬＨ１信号の２つの信号を出力する。

【００２６】

一方、第３の２帯域分割部１０３は、ダウンサンプラ１４１からの信号を入力し、垂直方向成分に関してＬＰＦ１１３およびＨＰＦ１２３によりそれぞれフィルタリングを行い、ダウンサンプラ１３３および１４３を用いて２：１に間引い

た後、ＨＬ１信号とＨＨ１信号の２つの信号を出力する。

【００２７】

これにより、第１の帯域分割フィルタ１００からは、水平方向・垂直方向共に低域のＬＬ１信号、水平方向に低域で垂直方向に高域のＬＨ１信号、水平方向に高域で垂直方向に低域のＨＬ１信号および水平方向・垂直方向共に高域のＨＨ１信号の４つの信号、すなわち、変換係数が出力される。なお、第２および第３の帯域分割フィルタ２００および３００も、入力する信号に対して上記と同様の処理を行う。

【００２８】

上述した第１～第３の帯域分割フィルタ１００、２００および３００による帯域分割処理の結果、画像信号７１は、ＬＬ３信号、ＬＨ３信号、ＨＬ３信号、ＨＨ３信号、ＬＨ２信号、ＨＬ２信号、ＨＨ２信号、ＬＨ１信号、ＨＬ１信号およびＨＨ１信号の１０個の周波数帯域に分割される。図６は、これらを２次元周波数領域で表現した図である。ここで、最も低い周波数帯域ＬＬ３信号をＭＲＡ、ＭＲＡ以外の周波数帯域をＭＲＲという。

【００２９】

つまり、ＭＲＲは、ＬＨ３信号、ＨＬ３信号、ＨＨ３信号、ＬＨ２信号、ＨＬ２信号、ＨＨ２信号、ＬＨ１信号、ＨＬ１信号およびＨＨ１信号を表している。図６において、縦軸は垂直方向の周波数成分を表し下側に行くほど高域となり、横軸は水平方向の周波数成分を表し右側に行くほど高域となる。

【００３０】

図６における各々の領域は１つの画像としてのデータであり、その領域の面積比は各々の帯域信号が有するデータ数の比に一致する。すなわち、第３の階層信号であるＬＬ３信号、ＬＨ３信号、ＨＬ３信号およびＨＨ３信号のデータ数を１とした場合、第２の階層信号であるＬＨ２信号、ＨＬ２信号およびＨＨ２信号のデータ数は４（２×２サイズ）となり、第１の階層信号であるＬＨ１信号、ＨＬ１信号およびＨＨ１信号のデータ数は１６（４×４サイズ）となる。

【００３１】

従って、例えば、ＬＬ３信号の左上の１個のデータに関しては、ＬＨ３信号、

ＨＬ３信号およびＨＨ３信号のそれぞれ左上の１個のデータが、ＬＨ２信号、ＨＬ２信号およびＨＨ２信号のそれぞれ左上の正方形の４個のデータが、ＬＨ１信号、ＨＬ１信号およびＨＨ１信号のそれぞれ左上の正方形の１６個のデータが原画像上での同一画素を表現することとなる（図６中、黒で塗りつぶしてある部分である）。つまり、画像信号において左上の正方形の６４個（８×８サイズ）の画素データは、上記の各周波数帯域の変換係数と同一の空間的領域を表現する。

【００３２】

次に、認証データ作成部１２は、予め定めた鍵データを用いて疑似乱数系列を作成し、当該疑似乱数系列から認証データを作成する（ステップＳ３０２）。具体的には、疑似乱数系列から生成されるランダムな実数値が正か負かを判断し、正の場合はビット値１と、負の場合はビット値０として認証データを作成する。鍵データとしては、例えば、疑似乱数系列を生成するための初期値、乱数発生関数の種類、系列のビット長を示す情報を含む。本実施の形態では、簡単のために各鍵データはそれぞれ８ビットのデータ長で表される値とする。また、以下の説明において、認証データは、ビット値１と０に２進数化されたビットストリームであるとする。鍵データの情報は、埋め込み処理を行うためのキー情報であり、情報を抽出する際にも用いるので、情報埋込み装置と情報抽出装置の双方側で予め値を決定しておく必要がある。

【００３３】

次に、鍵情報埋込み部１３は、帯域分割部１１で分割した信号のＭＲＡの変換係数を予め定めた順序で読み出し、前記鍵データを埋め込む（ステップＳ３０３）。この埋め込み手法として、特開平１１－１９６２６２号公報に開示された技術を用いる。すなわち、変換係数を量子化ステップサイズＱで割った値をｑとすると、変換係数に対応する鍵データのビット値に応じて、前記ｑの値を最も近い偶数または奇数の整数値に設定し、鍵データを埋め込むものである。なお、ＭＲＡの変換係数を読み出す予め定めた順序は、埋め込みを行うためのキー情報であり、鍵データを抽出する際にも用いる。また、鍵データを暗号化および誤り訂正符号を付加したデジタル情報に変換し、そのデジタル情報を埋め込むようにしてもよい。さらに、埋め込むデジタル情報のビット数が、ＭＲＡの変換係数より少

ない場合は、例えば、デジタル情報を一通り埋め込んだ後に当該デジタル情報の第１ビットに戻って引き続き埋め込む。

【００３４】

次に、認証データ埋込み部１４の処理（ステップＳ３０４）について図７を参照して説明する。図７は、認証データ埋込み部１４の一例を示すブロック図である。帯域分割部１１で分割した信号のＭＲＲの中から図４で示したＬＨ３の変換係数Ｗｉを予め定めた順序で読み出し、比較器５１に入力として与える。比較器５１では、変換係数の絶対値｜Ｗｉ｜が予め定めた設定値Ｔ以上であるか否かを判定する。

【００３５】

この判定において変換係数の絶対値が設定値Ｔ未満である場合には、第１の埋込み部５２において、認証データ作成部１２で作成した変換係数に対応する認証データのビット値に応じて、変換係数Ｗｉを小さな正の数ｍまたは－ｍに設定する（正の数ｍは設定値Ｔより小さな値である）。

【００３６】

これに対し、上記判定において変換係数の絶対値が設定値Ｔ以上である場合には、第２の埋込み部５３において鍵情報埋込み部１３と同様に、変換係数Ｗｉを量子化ステップサイズＱで割った値をｑとすると、変換係数に対応する認証データのビット値に応じて、ｑの値を最も近い偶数または奇数の整数値に設定する。

【００３７】

以上の処理を行い、変換係数Ｗｉに認証データのビット値を埋め込み、埋め込み処理された変換係数Ｗｉ’を作成する。

【００３８】

上記に続いて、ＬＨ２の変換係数を予め定めた順序で読み出し、比較器５１に入力として与える。以降の処理は、ＬＨ３の変換係数に対するものと同様である。なお、ここでは、ＬＨ３の変換係数に対する処理に続いて、ＬＨ２の変換係数に対する処理を行ったが、この処理の順序は、ＬＨ３の変換係数に対する処理を先に行ってもよい。ＬＨ３とＬＨ２の処理順序、およびＬＨ３、ＬＨ２の変換係数を読み出すための予め定めた順序は、埋め込み処理を行うためのキー情報であ

り、情報を抽出する際にも用いる。また、ＬＨ２とＬＨ３の変換係数を比較する設定値Ｔは、必ずしも同一でなくてもよい。好ましくは、ＬＨ３の変換係数を比較する設定値は、ＬＨ２の変換係数を比較する設定値より小さくする方がよい。例えば、ＬＨ３の変換係数を比較する設定値は７、ＬＨ２の変換係数を比較する設定値は１０、ｍは２などと決めておく。

【００３９】

次に、帯域合成部１５の処理について、図８および図９を用いて説明する。図８は、図１の帯域合成部１５の構成の一例を示すブロック図である。帯域合成部１５は、それぞれ同じ構成を有する第１～第３の帯域合成フィルタ４００、５００および６００を備える。第１～第３の帯域合成フィルタ４００、５００および６００は、４つの周波数帯域信号を入力し、１つの信号に合成して出力する（ステップＳ３０５）。

【００４０】

第１の帯域合成フィルタ４００は、ＬＬ３信号、ＬＨ３信号、ＨＬ３信号およびＨＨ３信号とを入力し、これらを合成してＬＬ２信号を作成する。第２の帯域合成フィルタ５００は、上記合成したＬＬ２信号とＬＨ２信号、ＨＬ２信号およびＨＨ２信号とを入力し、これらを合成してＬＬ１信号を作成する。そして、第３の帯域合成フィルタ６００は、上記合成したＬＬ１信号とＬＨ１信号、ＨＬ１信号およびＨＨ１信号とを入力し、これらを合成してデジタル画像信号７２を再構成する。

【００４１】

図９は、第１の帯域合成フィルタ４００の構成の一例を示すブロック図である。図９において、第１の帯域合成フィルタ４００は、第１～第３の２帯域合成部４０１～４０３を備える。この第１～第３の２帯域合成部４０１～４０３は、それぞれＬＰＦ４１１～４１３と、ＨＰＦ４２１～４２３と、信号に対して２：１の割合で零を挿入するアップサンプラ４３１～４３３および４４１～４４３と、加算器４５１～４５３とを備える。

【００４２】

第１の２帯域合成部４０１は、ＬＬ３信号とＬＨ３信号とを入力して、それぞ

れアップサンプラ４３１および４４１を用いて２倍のサイズの信号に変換し、変換した２つの信号を垂直方向成分に関してＬＰＦ４１１およびＨＰＦ４２１でフィルタリングした後、加算して出力する。

【００４３】

一方、第２の２帯域合成部４０２は、ＨＬ３信号とＨＨ３信号とを入力して、それぞれアップサンプラ４３２および４４２を用いて２倍のサイズの信号に変換し、変換した２つの信号を垂直方向成分に関してＬＰＦ４１２およびＨＰＦ４２２でフィルタリングした後、加算して出力する。

【００４４】

そして、第３の２帯域合成部４０３は、加算器４５１および４５２の出力を入力して、それぞれアップサンプラ４３３および４４３を用いて２倍のサイズの信号に変換し、変換した２つの信号を水平方向成分に関してＬＰＦ４１３およびＨＰＦ４２３でフィルタリングした後、加算して出力する。

【００４５】

これにより、第１の帯域合成フィルタ４００からは、第２の階層信号である水平・垂直方向共に低域のＬＬ２信号が出力される。なお、第２および第３の帯域合成フィルタ５００および６００も、入力する信号に対して上記と同様の処理を行う。帯域合成部１５は、上述のようにＬＬ３信号、ＬＨ３信号、ＨＬ３信号、ＨＨ３信号、ＬＨ２信号、ＨＬ２信号、ＨＨ２信号、ＬＨ１信号、ＨＬ１信号およびＨＨ１信号の１０個の周波数帯域信号を、埋め込み処理が行われたデジタル画像信号７２に再構成して出力する。

【００４６】

次に、情報抽出装置２ａが行う情報抽出方法について図２と図１０を参照して説明する。図１０は、図２の情報抽出装置２ａで行う処理を示すフローチャートである。帯域分割部１１は、デジタル画像信号７３を入力する。このデジタル画像信号７３は、上記情報埋込み装置１ａの帯域合成部１５が出力するデジタル画像信号７２が送信途中で、圧縮符号化・伸長化の処理、あるいは改ざん処理が施された信号である。帯域分割部１１は、入力されたデジタル画像信号７３に関して離散ウェーブレット変換を行って１０個の周波数帯域ＬＬ３信号、ＬＨ３信号

、ＨＬ３信号、ＨＨ３信号、ＬＨ２信号、ＨＬ２信号、ＨＨ２信号、ＬＨ１信号、ＨＬ１信号およびＨＨ１信号に分割し、それぞれの変換係数を算出する（ステップＳ１００１）。

【００４７】

次に、鍵情報抽出部２１は、帯域分割部１１で分割したＭＲＡ成分の変換係数から情報埋込み装置１ａの鍵情報埋込み部１３で行ったのと同じ順序で読み出し、埋め込まれている鍵情報を抽出する（ステップＳ１００２）。この抽出手法は、特開平１１－１９６２６２号公報に開示された技術を用いる。すなわち、変換係数を量子化ステップサイズＱで割った値を四捨五入した値をｐとすると、前記ｐの値が偶数か奇数かを判定し、当該判定の結果に基づいて埋込まれた情報のビット値を抽出する。

【００４８】

次に、鍵情報判定部２２は、鍵情報抽出部２１で抽出した情報が、情報埋込み装置１ａにおいて用いた鍵データと同一であるか否かの正当性を判定する（ステップＳ１００３）。例えば、鍵データに含まれる初期値、乱数発生関数の種類、系列のビット長の各値をそれぞれ情報埋込み装置と情報抽出装置の双方で予め複数個の候補を決めておく。

【００４９】

もし抽出した情報がその候補値といずれも一致しない場合、同一でないと判定するようにする。このステップＳ１００３における判定の結果、正しいと判断した場合は、ステップＳ１００４以降の処理を行う。一方、ステップＳ１００３における判定の結果、正しくないと判断した場合は、デジタル画像信号７３には改ざん有りと検出する（ステップＳ１０１１）。

【００５０】

この判定部は必須ではないが、鍵データの正当性を判定することにより、本発明の改ざん防止装置における信頼性が増して、実用上好ましい。次に、認証データ作成部１２は、前記鍵データを用いて疑似乱数系列を作成し、当該疑似乱数系列から認証データＫを作成する（ステップＳ１００４）。

【００５１】

次に、埋込み情報抽出部２３の処理（ステップＳ１００５）について図２と図１１を参照して説明する。図１１は、埋込み情報抽出部２３の一例を示すブロック図である。帯域分割部１１で分割したＭＲＲ成分の中からＬＨ３、ＬＨ２の変換係数を情報埋込み装置１ａの認証データ埋込み部１４で行ったのと同じ順序、すなわち、ＬＨ３、ＬＨ２の順に認証データ埋込み部１４と同一の予め定めた順序で読み出す。読み出された変換係数Ｗｉは、比較器５１に入力され、変換係数の絶対値｜Ｗｉ｜が予め定めた設定値Ｔ以上であるか否かを判定する。

【００５２】

この判定において変換係数の絶対値が設定値Ｔ未満である場合には、第１の抽出部５４において、変換係数の値が正か負かを判定し、当該判定の結果に基づいて変換係数毎に埋込まれた埋込み情報のビット値を抽出する。

【００５３】

これに対し、変換係数の絶対値が設定値Ｔ以上である場合には、第２の抽出部５５において、上記鍵情報抽出部２１と同様に、変換係数を量子化ステップサイズＱで割り四捨五入した値をｐとすると、前記ｐの値が偶数か奇数かを判定し、当該判定の結果に基づいて変換係数毎に埋込まれた埋込み情報のビット値を抽出する。以上の処理を行い、埋込み情報Ｄを抽出する（ステップＳ１００５）。

【００５４】

次に、領域対応埋込情報読出部２４と領域対応認証データ読出部２５の処理について、図２と図１２を参照して説明する。図１２は、デジタル画像信号７３を３２×３２画素サイズのブロックに分割した場合、画像中の左上のブロックと同一の空間的領域を表現するＬＨ３とＬＨ２の変換係数を示している（図１２中の太い実線の枠線部分に対応する）。

【００５５】

すなわち、ＬＨ３とＬＨ２の各ブロックサイズは、それぞれ縦横４×４画素、８×８画素である。今、ＬＨ３、ＬＨ２の変換係数を読み出す予め定めた順序が、縦横１つ毎に読み出した場合、ＬＨ３内の４個とＬＨ２内の１６個が各ブロックの位置と同一の空間的領域を表現する変換係数内に埋め込まれている埋込み情報の系列である（図１２中、黒で塗りつぶした部分である）。

【００５６】

従って、領域対応埋込情報読出部２４では、埋込み情報抽出部２３で抽出した埋込み情報Ｄの中から、上記２０個の埋込み情報の系列ＢＤを読み出す（ステップＳ１００６）。

【００５７】

同様に、領域対応認証データ読出部２５では、認証データ作成部１２で作成した認証データＫの中から、埋込み情報の系列ＢＤと同じ位置に対応する２０個の認証データの系列ＢＫを読み出す（ステップＳ１００７）。

【００５８】

例えば、図１２において、ＬＨ３とＬＨ２の左上のブロックに埋め込まれている埋込み情報の系列ＢＤが、ＢＤ＝｛１，０，１，１，１，０，０，１，１，０，０，１，１，１，０，１，０，１，０，１｝で、認証データの系列ＢＫが、ＢＫ＝｛１，１，１，０，１，０，０，１，１，０，０，０，１，０，０，１，０，１，０，１｝であるとする。この例では、２、４、１２、１４番目のビットが４箇所異なっている。

【００５９】

次に、ブロック改ざん判定部２６は、上記読み出したビット列ＢＤとＢＫとの排他的論理和の総和を求める（ステップＳ１００８）。

【００６０】

その求めた値Ｓと予め定めた設定値ＢＴを比較することにより、ブロックに分割した部分画像（ここでは、３２×３２画素サイズのブロック）に対して改ざんが行われている否かを判定する（ステップＳ１００９）。

【００６１】

例えば、求めた値Ｓが予め定めた設定値ＢＴより大きい場合は、改ざんが行われていると判定し、反対に小さい場合は、改ざんが行われていないと判定する。排他的論理和の例を説明したのが図１３である。お互いのビットの値が相異なる場合は値１を出力し、同じビット値同士の場合は値０を出力する。上記のビット列ＢＤとＢＫに適用した場合、出力値Ｓは４となる。予め定めた設定値ＢＴが３である場合は、値Ｓが設定値Ｔより大きいため、当該ブロックは改ざんが行われ

ていると判定される。

【００６２】

なお、排他的論理和の総和を求める代わりに、ビット列ＢＤとＢＫの２０個のビット値の一致している個数または内積を求めて比較してもよい。また、ビット値を０のかわりに－１として内積を計算してもよい。このステップＳ１００９における判定の結果、改ざんが有ると判断した場合は、前記ブロックに対応する位置を改ざん有りとメモリに格納（図示せず）またはディスプレイに表示（図示せず）する（ステップＳ１０１１）。

【００６３】

一方、ステップＳ１００９における判定の結果、改ざんが無いと判断した場合は、前記ブロックに対応する位置を改ざん無しとメモリに格納（図示せず）またはディスプレイに表示（図示せず）する（ステップＳ１０１０）。

【００６４】

以上のステップＳ１００６からステップＳ１００９の処理を、全てのブロックに対して繰り返し行うことにより、デジタル画像中の改ざん部分の位置を検出する。

【００６５】

以上のように、本実施形態に係る改ざん防止装置によれば、３階層に帯域分割を行い、ＭＲＲの中からＬＨ３、ＬＨ２の全体の変換係数に認証データを埋め込む。しかも、認証データは、鍵データを用いて疑似乱数系列から作成し、その鍵データはＭＲＡの変換係数に埋め込む。さらに、画像を予め定めた複数の画素から構成される複数のブロックに分割し、各ブロックと同一の空間的領域を表現するＭＲＲの変換係数内に埋め込んだ埋込み情報を読み出し、実際に埋め込んだ認証データと比較照合することにより、デジタル画像中の改ざん部分の位置を検出することができる。

【００６６】

従って、比較的低周波成分の変換係数に情報を埋込むことにより、非可逆的な圧縮符号化を行っても埋め込んだ鍵データと認証データは保持される。すなわち、非可逆的な圧縮と画像の一部を改ざんする行為とを区別することができ、しか

も改ざん部分の特定が可能なデジタル画像の改ざん防止装置を実現できる。

【００６７】

なお、本実施形態に係る改ざん防止装置において行う離散ウェーブレット変換は、３つの階層に限られるものではなく、ＬＬ信号が１×１の要素になるまで何回でも階層化してよい。また、認証データを埋め込みに用いる帯域はＬＨ３、ＬＨ２に限ったものではなく、ＭＲＲの中から任意の帯域を選択して用いてもよく、またＭＲＲ全域を用いてもよい。この場合、帯域の変換係数に対する処理の順序は、いずれの順序でもよいが、その順序は予め定めておく必要がある。

【００６８】

ただし、本発明においては、より深い階層信号のみの変換係数に認証データを埋め込むのが最も好ましく、例えば、図４において、第３の階層信号のＬＨ３信号とＨＬ３信号、第２の階層信号のＬＨ２信号とＨＬ２信号の全てもしくはその一部から構成した数列に埋め込むようにしている。

【００６９】

また、認証データは、認証データ埋込み部１４において予め定めた順序で読み出された変換係数毎に順番に埋め込むようにしているが、複数のブロックに分割した各ブロックと同一の空間的領域を表現するＭＲＲ内に埋め込む認証データは、ブロック毎に同じ認証データを繰り返し埋め込むようにしてもよい。

【００７０】

なお、情報埋込み装置において鍵データを公開鍵暗号または共通鍵暗号を行って暗号化して埋め込み、情報抽出装置において暗号化された情報を復号する場合は、両装置間で予め公開鍵または共通鍵を決定しておく必要がある。

【００７１】

なお、典型的には、上記の実施形態に係る改ざん防止装置が実現する各機能は、所定のプログラムデータが格納された記憶装置（ＲＯＭ，ＲＡＭ，ハードディスク等）と、当該プログラムデータを実行するＣＰＵ（セントラル・プロセッシング・ユニット）とによって実現される。この場合、各プログラムデータは、ＣＤ－ＲＯＭやフロッピーディスク等の記録媒体を介して導入されてもよい。

【００７２】

【発明の効果】

本発明によれば、デジタル画像中のどの位置が改ざんされたのかを領域別に特定することができる。また、非可逆的な圧縮符号化を行っても埋め込んだ鍵データと認証データが保持されるので、非可逆的な画像圧縮と画像の一部を改ざんするような行為とを区別することができる。しかも、埋め込まれた周波数帯域の情報、具体的に用いた変換係数、変換係数の読み出し順序、および鍵データの情報を知らない第三者による認証データの解読が困難なため、埋め込み情報の上書きやすり替えは不可能である。

【図面の簡単な説明】

【図１】

本発明の実施形態に係る改ざん防止装置の情報埋込み装置の構成図

【図２】

本発明の実施形態に係る改ざん防止装置の情報抽出装置の構成図

【図３】

図１の情報埋込み装置で行う処理のフローチャート

【図４】

図１の帯域分割部の構成を示すブロック図

【図５】

図４の第１の帯域分割フィルタの構成を示すブロック図

【図６】

離散ウェーブレット変換による各信号の２次元周波数領域での表現図

【図７】

図１の認証データ埋込み部の構成を示すブロック図

【図８】

図１の帯域合成部の構成を示すブロック図

【図９】

図８の第１の帯域合成フィルタの構成を示すブロック図

【図１０】

図２の情報抽出装置で行う処理のフローチャート

【図１１】

図２の埋込み情報抽出部の構成を示すブロック図

【図１２】

３２×３２画素サイズのブロックと同一の空間的領域を表現するＬＨ３とＬＨ２の変換係数の模式図

【図１３】

排他的論理和の例の説明図

【図１４】

従来の電子認証手順の説明図

【符号の説明】

１ａ　情報埋込み装置

２ａ　情報抽出装置

１１　帯域分割部

１２　認証データ作成部

１３　鍵情報埋込み部

１４　認証データ埋込み部

１５　帯域合成部

２１　鍵情報抽出部

２２　鍵情報判定部

２３　埋込み情報抽出部

２４　領域対応埋込情報読出部

２５　領域対応認証データ読出部

２６　ブロック改ざん判定部

５１　比較器

５２　第１の埋込み部

５３　第２の埋込み部

５４　第１の抽出部

５５　第２の抽出部

７１，７２，７３　デジタル画像信号

１００，２００，３００　帯域分割フィルタ

１０１～１０３　２帯域分割部

１１１～１１３，４１１～４１３　１次元の低域通過フィルタ（ＬＰＦ）

１２１～１２３，４２１～４２３　１次元の高域通過フィルタ（ＨＰＦ）

１３１～１３３，１４１～１４３　ダウンサンプラ

４００，５００，６００　帯域合成フィルタ

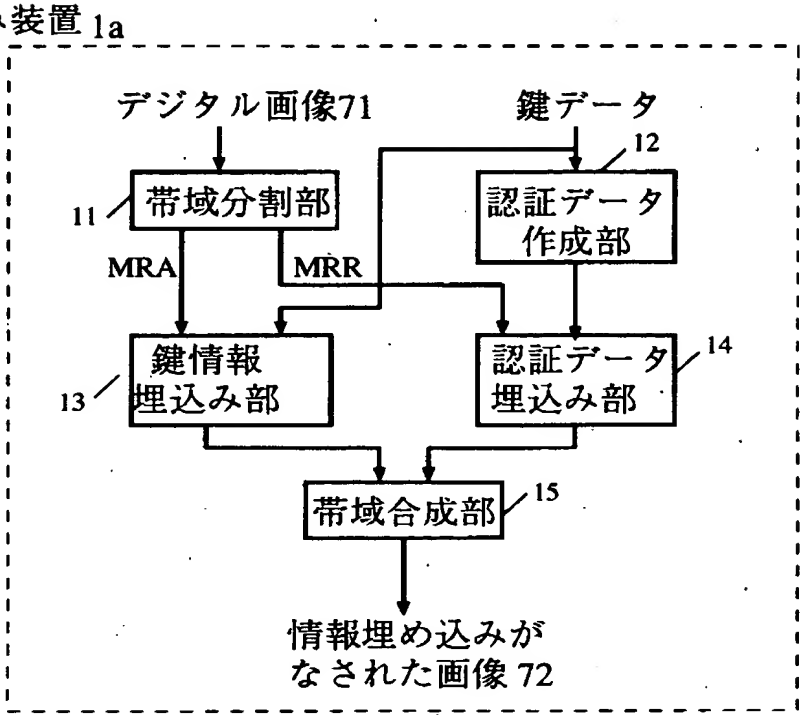
４０１～４０３　２帯域合成部

４３１～４３３，４４１～４４３　アップサンプラ

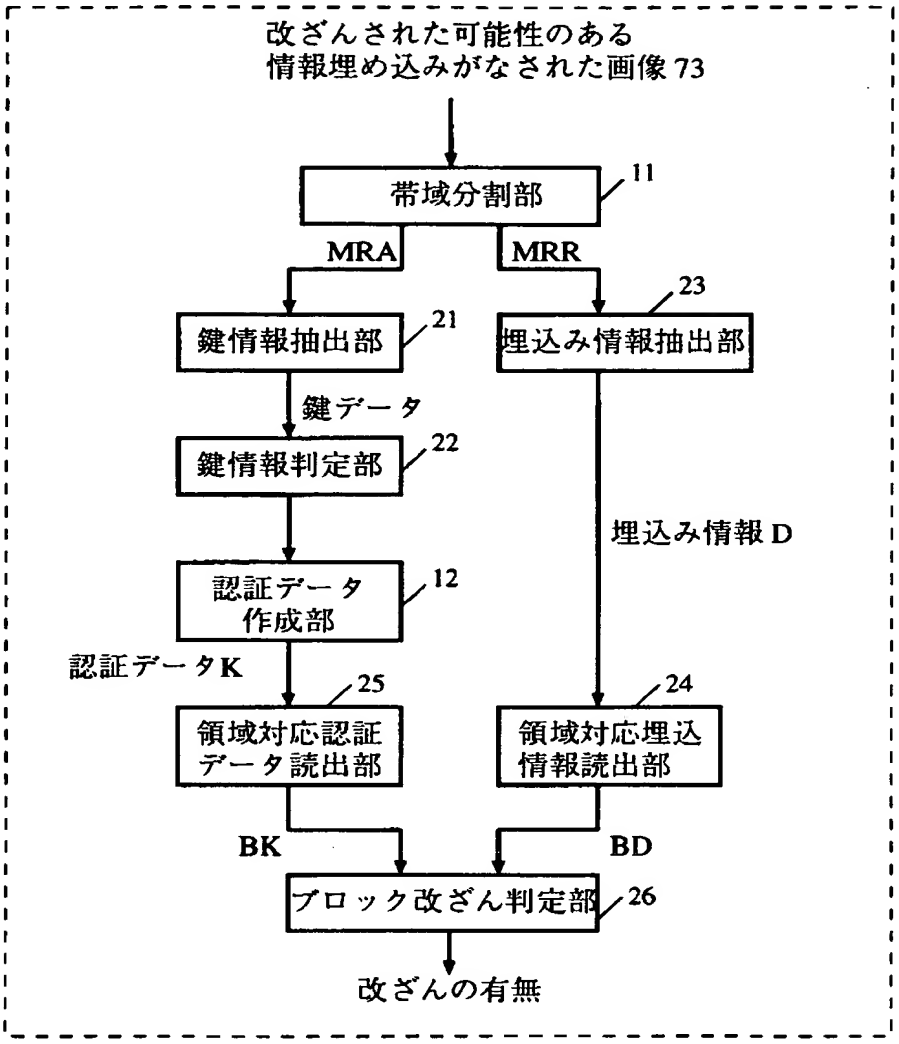
４５１～４５３　加算器

【書類名】　図面

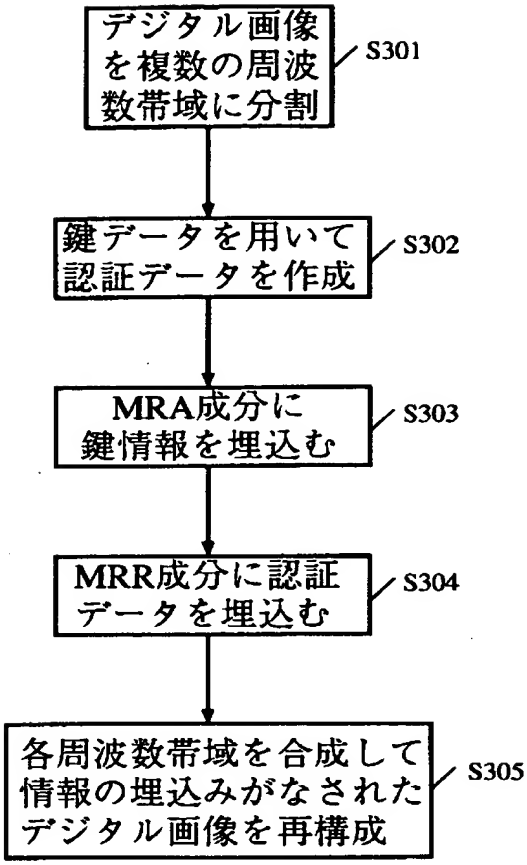
【図１】


情報埋込み装置 1a
デジタル画像71
鍵データ
12
11
帯域分割部
認証データ作成部
MRA
MRR
鍵情報埋込み部
13
認証データ埋込み部
14
帯域合成部
15
情報埋め込みがなされた画像 72

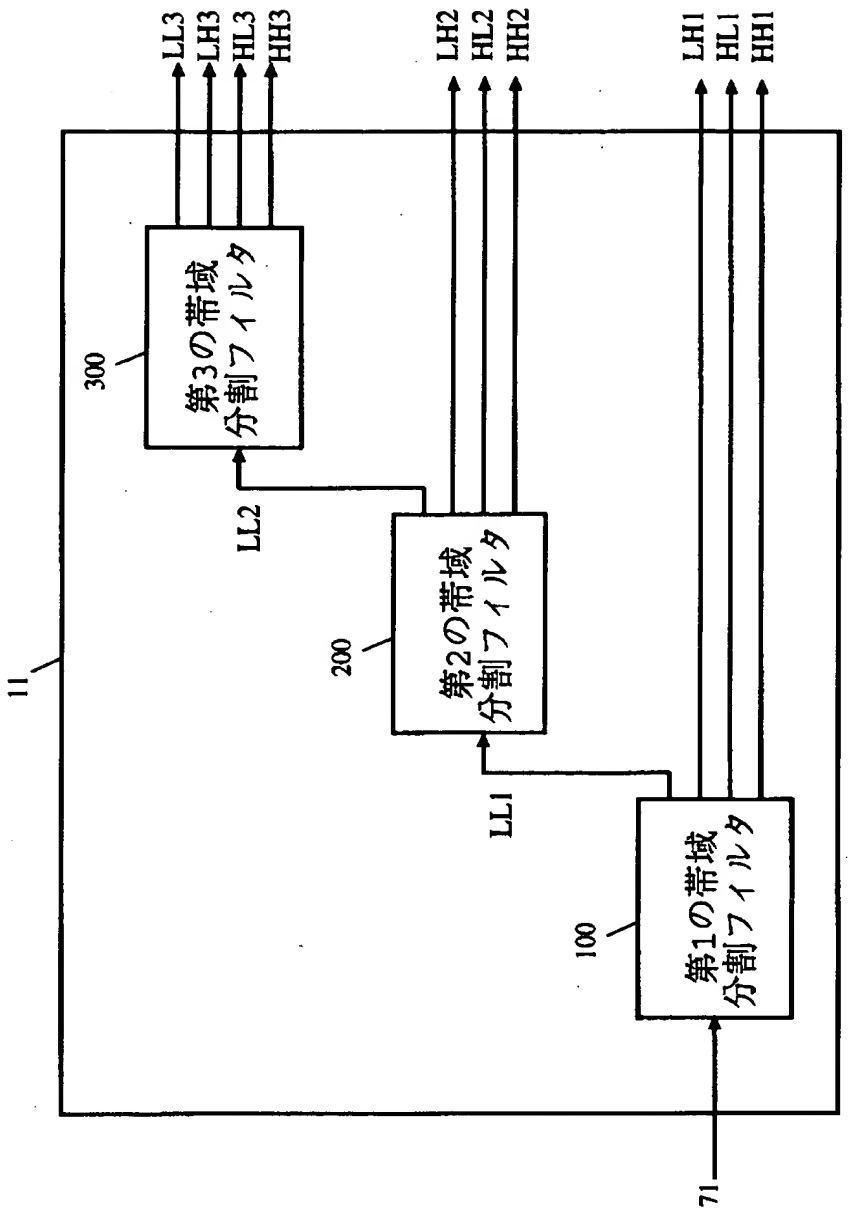
【図２】


情報抽出装置2a
改ざんされた可能性のある
情報埋め込みがなされた画像 73
帯域分割部
11
MRA
MRR
鍵情報抽出部
21
埋込み情報抽出部
23
鍵データ
鍵情報判定部
22
埋込み情報 D
認証データ
作成部
12
認証データK
領域対応認証
データ読出部
25
領域対応埋込
情報読出部
24
BK
BD
ブロック改ざん判定部
26
改ざんの有無

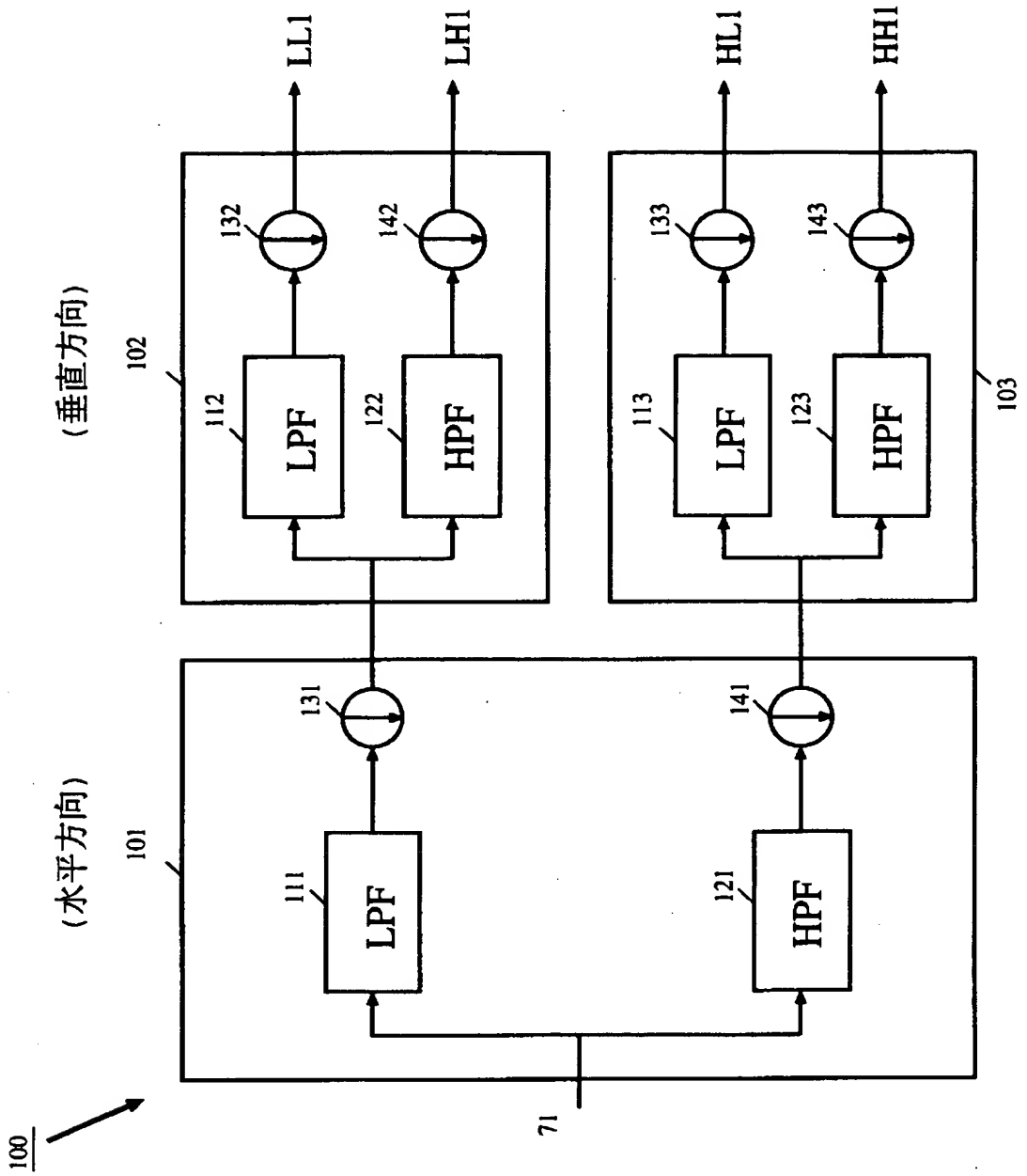
【図３】


デジタル画像を複数の周波数帯域に分割
S301
鍵データを用いて認証データを作成
S302
MRA成分に鍵情報を埋込む
S303
MRR成分に認証データを埋込む
S304
各周波数帯域を合成して情報の埋込みがなされたデジタル画像を再構成
S305

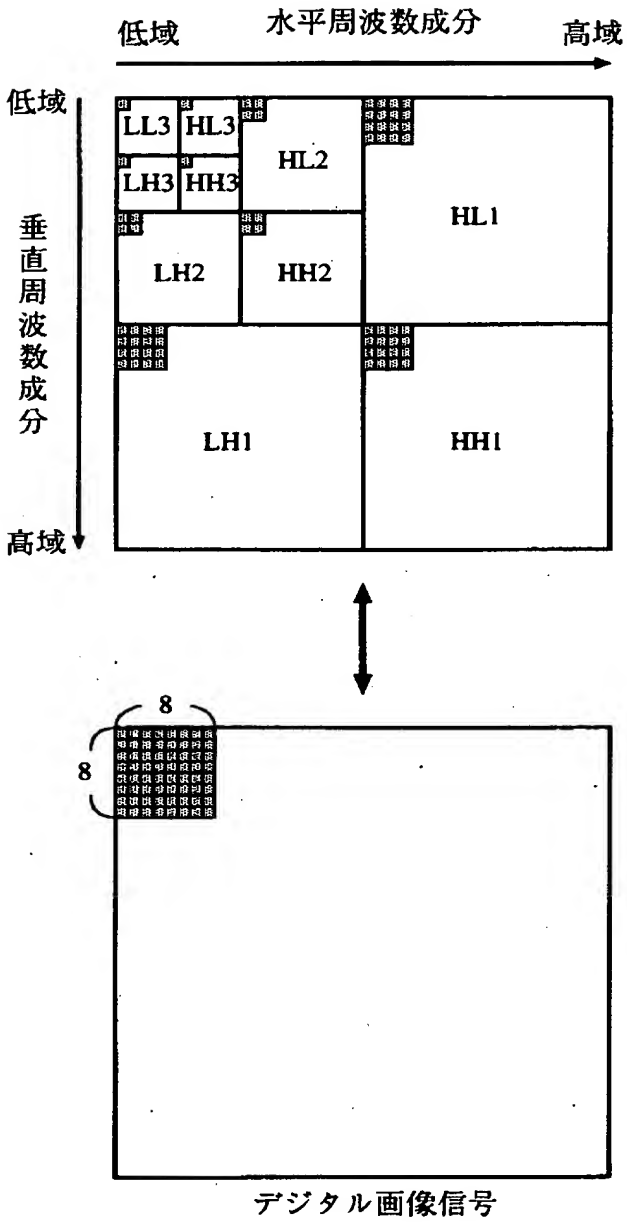
【図４】


LL3
LH3
HL3
HH3
LH2
HL2
HH2
LH1
HL1
HH1
300
第3の帯域分割フィルタ
LL2
200
第2の帯域分割フィルタ
LL1
100
第1の帯域分割フィルタ
11
71

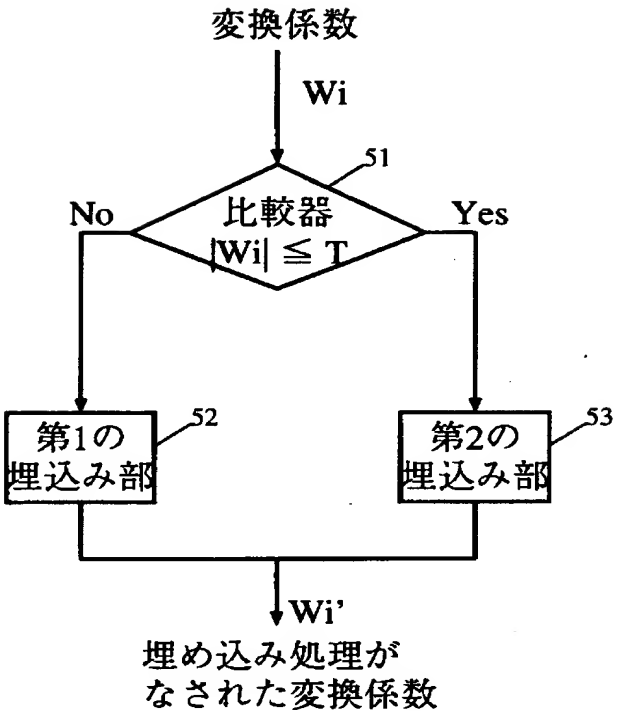
【図５】


LL1
LH1
HL1
HH1
(垂直方向)
(水平方向)
102
103
101
132
142
133
143
131
141
112
122
113
123
111
121
LPF
HPF
LPF
HPF
LPF
HPF
100
71

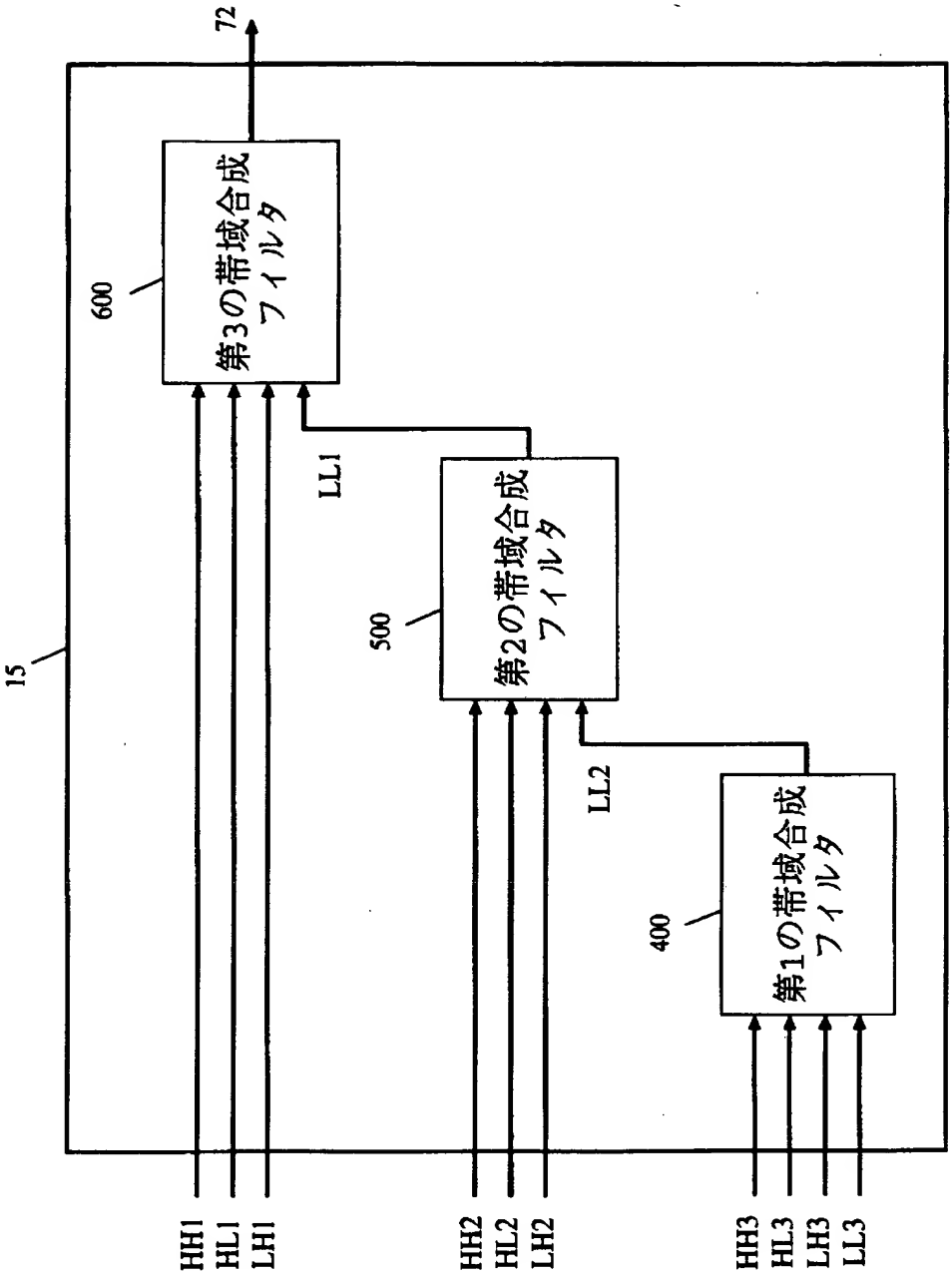
【図６】


低域
水平周波数成分
高域
低域
垂直周波数成分
高域
LL3
HL3
HL2
LH3
HH3
HL1
LH2
HH2
LH1
HH1
8
8
デジタル画像信号

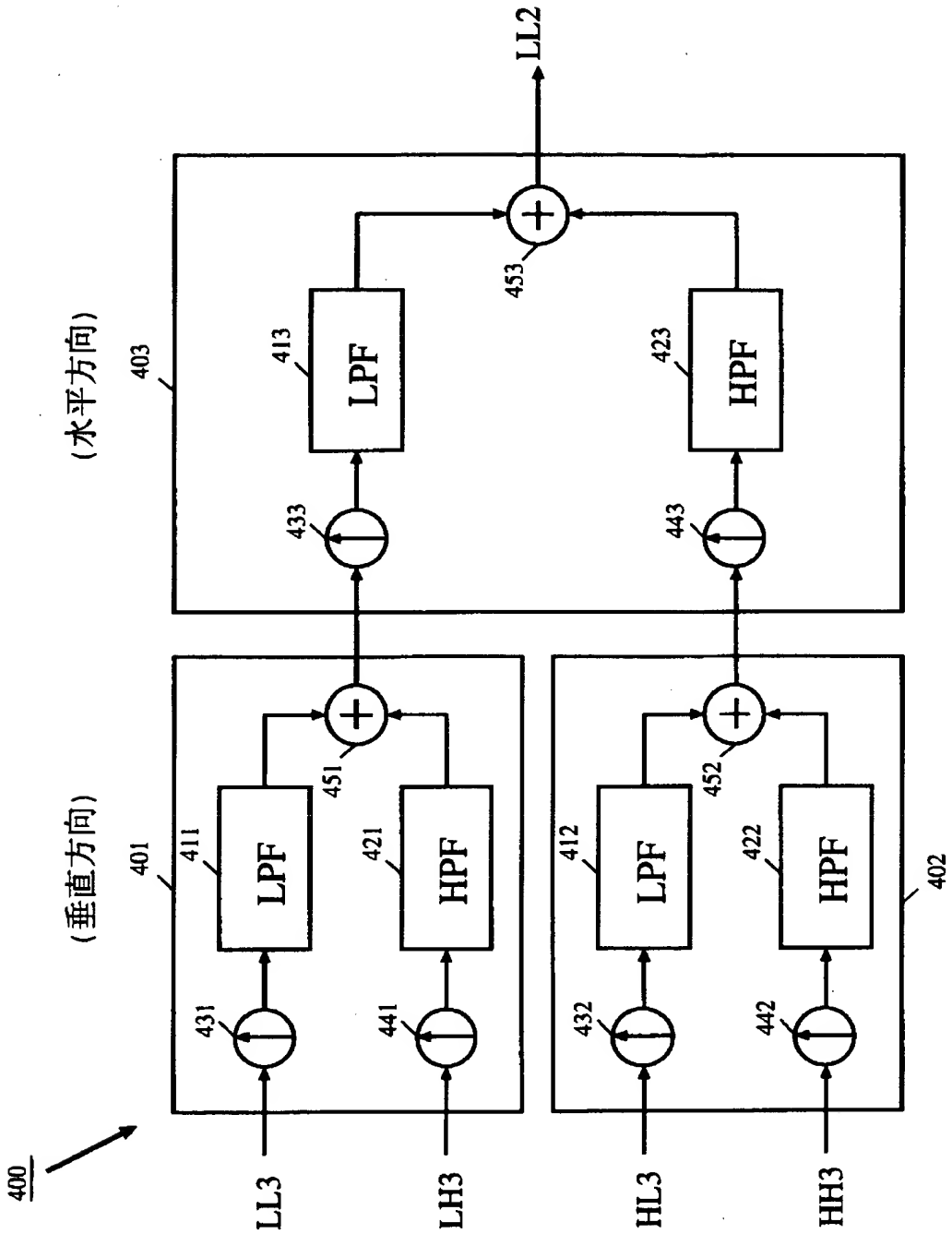
【図７】


変換係数
Wi
51
比較器
|Wi| ≦ T
No
Yes
第1の
埋込み部
52
第2の
埋込み部
53
Wi'
埋め込み処理が
なされた変換係数

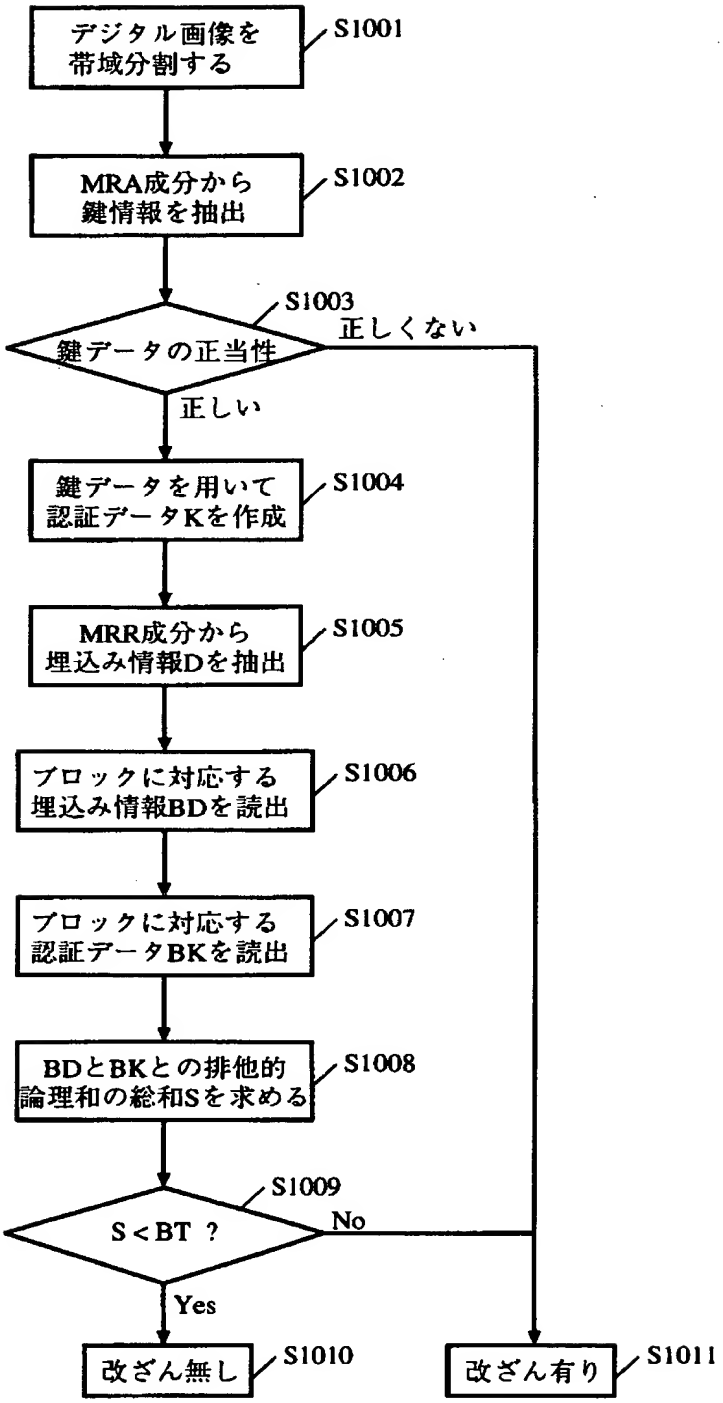
【図８】


72
第3の帯域合成フィルタ
600
LL1
第2の帯域合成フィルタ
500
LL2
第1の帯域合成フィルタ
400
15
HH1
HL1
LH1
HH2
HL2
LH2
HH3
HL3
LH3
LL3

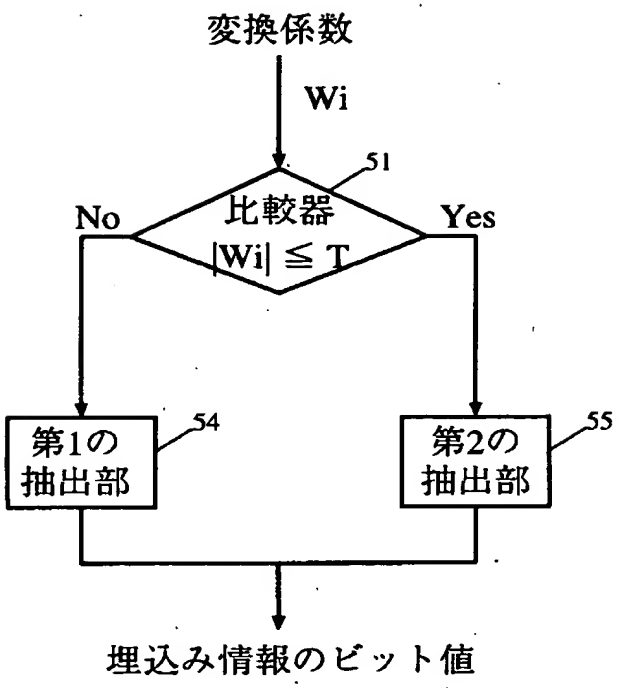
【図９】


400
LL3
LH3
HL3
HH3
(垂直方向)
401
402
403
411
412
413
421
422
423
431
432
433
441
442
443
451
452
453
LPF
HPF
LL2
(水平方向)

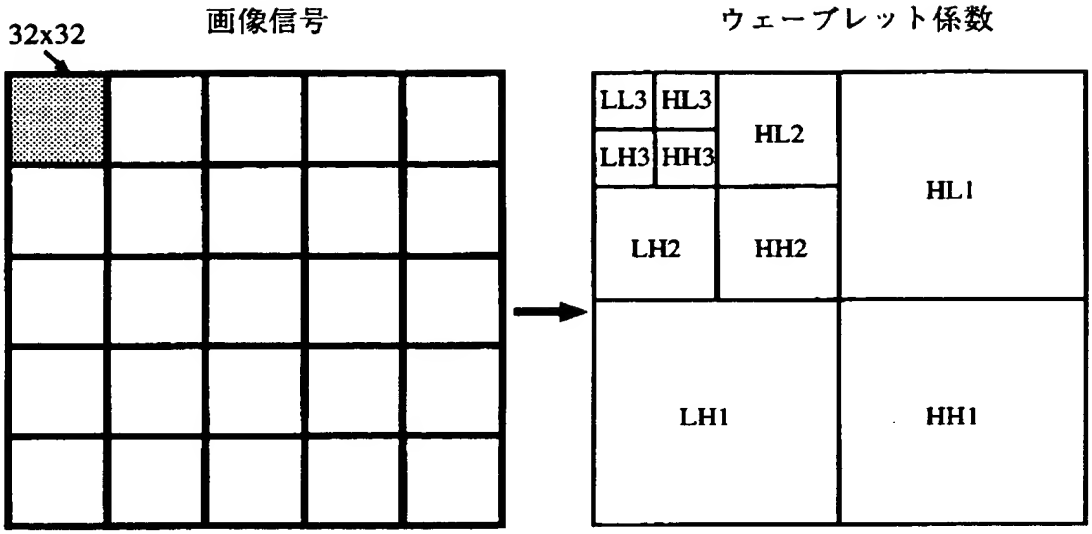
【図１０】

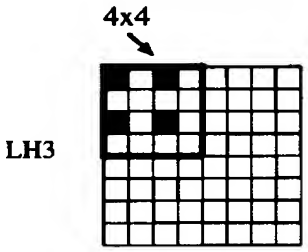

デジタル画像を
帯域分割する
S1001
MRA成分から
鍵情報を抽出
S1002
S1003
鍵データの正当性
正しくない
正しい
鍵データを用いて
認証データKを作成
S1004
MRR成分から
埋込み情報Dを抽出
S1005
ブロックに対応する
埋込み情報BDを読出
S1006
ブロックに対応する
認証データBKを読出
S1007
BDとBKとの排他的
論理和の総和Sを求める
S1008
S1009
S < BT ?
No
Yes
改ざん無し
S1010
改ざん有り
S1011

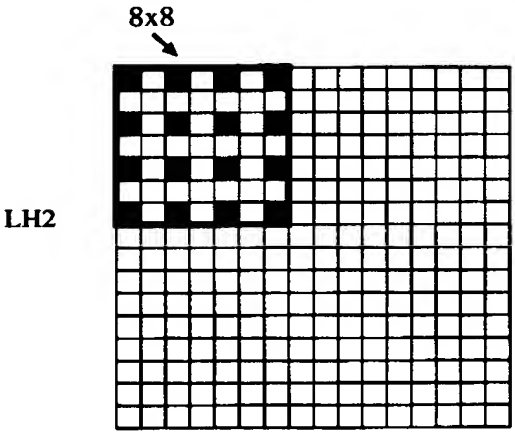
【図１１】



【図１２】


32x32
画像信号
ウェーブレット係数
LL3
HL3
LH3
HH3
HL2
HL1
LH2
HH2
LH1
HH1

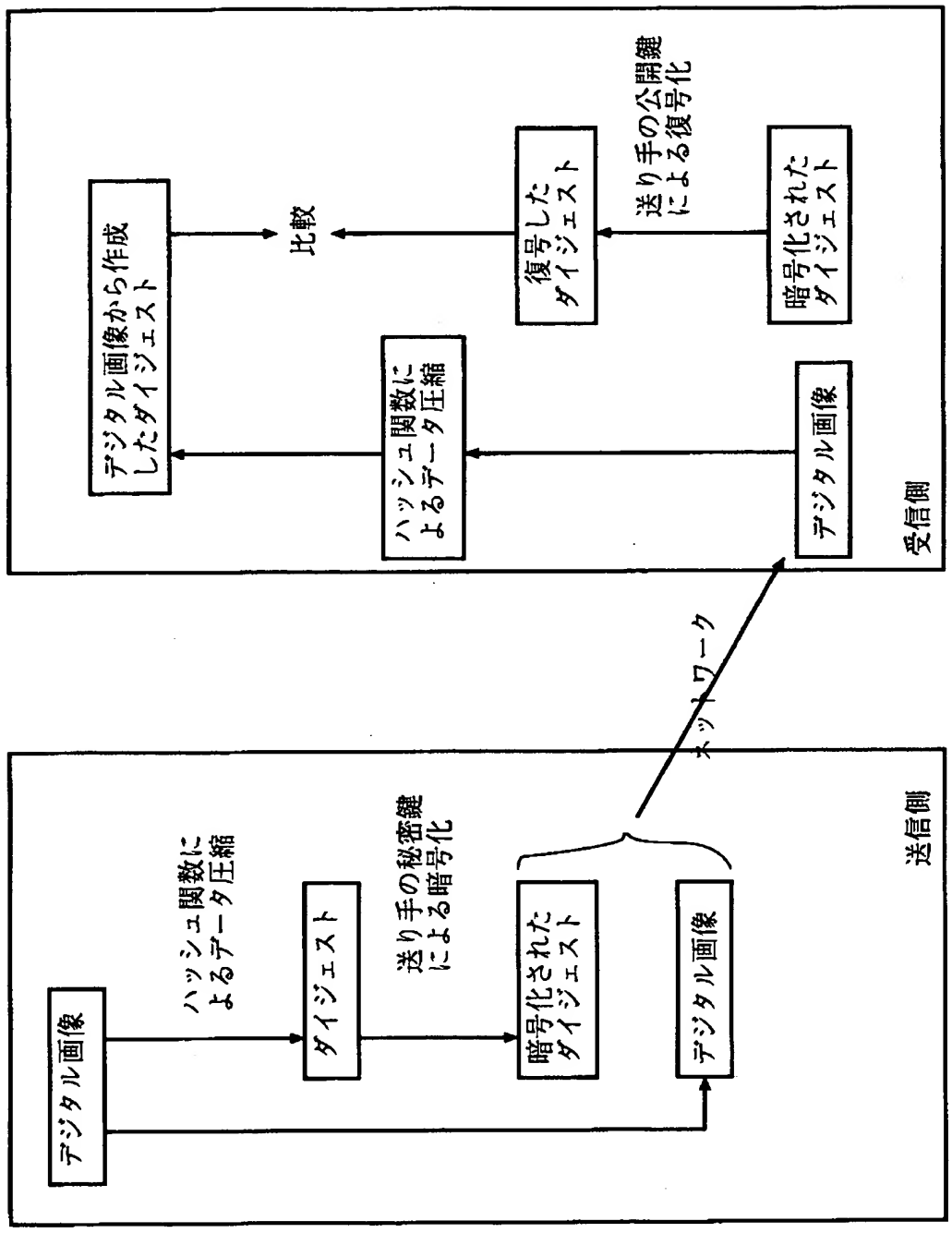

4x4
LH3


8x8
LH2

【図１３】

0 x 0 = 0
0 x 1 = 1
1 x 0 = 1
1 x 1 = 0

【図１４】


送信側
デジタル画像
ハッシュ関数によるデータ圧縮
ダイジェスト
送り手の秘密鍵による暗号化
暗号化されたダイジェスト
デジタル画像
ネットワーク
受信側
デジタル画像
ハッシュ関数によるデータ圧縮
暗号化されたダイジェスト
送り手の公開鍵による復号化
復号したダイジェスト
比較
デジタル画像から作成したダイジェスト

【書類名】　要約書

【要約】

【課題】　画像圧縮と改ざん行為とを区別でき、画像中のどの位置が改ざんされたのかを領域別に特定することができる。

【解決手段】　情報埋込み装置では、画像を複数の周波数帯域に分割し変換係数を算出する。鍵データを用いて疑似乱数系列を作成し認証データを作成する。鍵データはＭＲＡ、認証データはＭＲＲの変換係数に埋込む。埋込み処理されたＭＲＡとＭＲＲを合成し情報が埋込まれた画像を再構成する。情報抽出装置では、画像を帯域分割したＭＲＡから鍵データを抽出し、本来埋込んである認証データを作成する。ＭＲＲから埋込み情報を抽出する。画像を予め定めた複数の画素から構成される複数のブロックに分割し、各ブロックと同一の空間的領域を表現するＭＲＲの変換係数内に埋込まれている埋込み情報の系列とそれに対応する認証データの系列とを比較照合することにより、領域毎の改ざんの有無を判定する。

【選択図】　図２

出　願　人　履　歴　情　報

識別番号　　〔０００００５８２１〕

１．変更年月日　　１９９０年　８月２８日
［変更理由］　新規登録
住　所　　大阪府門真市大字門真１００６番地
氏　名　　松下電器産業株式会社